UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/556,247	11/10/2005	Srinivas Gutta	US030119	3675

24737 7590 02/09/2009
PHILIPS INTELLECTUAL PROPERTY & STANDARDS
P.O. BOX 3001
BRIARCLIFF MANOR, NY 10510

EXAMINER	
JIANG, YONG HANG	
ART UNIT	PAPER NUMBER
2612	

MAIL DATE	DELIVERY MODE
02/09/2009	PAPER

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Office Action Summary	Application No.	Applicant(s)	
	10/556,247	GUTTA ET AL.	
	Examiner	Art Unit	
	YONG HANG JIANG	2612	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *10 November 2005*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *10 November 2005* is/are: a)☒ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☒ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date *11/10/2005*.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

Claim Rejections - 35 USC § 112

1. The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

2. Claim 2, 4, 6, 8, 14, 16, 18, 20, and 22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Regarding the claims, the phrase "comparatively more sophisticated sensor" on line 2 of the claims rendered the claims indefinite, it is unclear how and in what way the sensor is more sophisticated.

Claim Rejections - 35 USC § 102

3. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (e) the invention was described in (1) an application for patent, published under section 122(b), by another filed in the United States before the invention by the applicant for patent or (2) a patent granted on an application for patent by another filed in the United States before the invention by the applicant for patent, except that an international application filed under the treaty defined in section 351(a) shall have the effects for purposes of this subsection of an application filed in the United States only if the international application designated the United States and was published under Article 21(2) of such treaty in the English language.

4. Claims 1-2 and 13-14 are rejected under 35 U.S.C. 102(e) as being anticipated by Nikolsky (US 2003/0068044).

Regarding claim 1, Nikolsky discloses a method for selectively activating biometric sensors (Fig. 1) to authenticate the identity of an individual (See paragraphs 34-38, Figure 2), comprising:

activating a first tier biometric sensor (via finger print sensor 15, See Figure 1) to verify the biometric of said individual (Paragraph 37); and

activating a second tier biometric sensor to verify the biometric of said individual in the case where said individual is successfully verified with said first tier biometric sensor (via biometric sensor 20, See paragraph 38).

Regarding claim 13, Nikolsky discloses a system (See Figure 1) comprising:

a biometric security device (via Yoke handgrip 10, Figure 1) comprising a plurality of biometric devices;

at least one processor (via processor 35, Figure 1) connected to said biometric security device , said at least one processor including one or more databases (via digitized fingerprint database 45, Figure 1) for storing biometric and user data;

said processor programmed to process the method disclosed in claim 1 above (Therefore, the claimed limitations are rejected for the same reasons as claim 1 above).

Regarding claims 2 and 14, Nikolsky discloses the second tier biometric sensor is more sophisticated than the first biometric sensor (via the biometric sensor to sense distress experienced by a pilot, See paragraph 8).

5. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

6. Claim 3-4 and 15-16 is rejected under 35 U.S.C. 102(b) as being anticipated by Ikegami et al. (US 6,983,061).

Regarding claim 3, Ikegami discloses a method for selectively activating biometric sensors to authenticate the identity of an individual while conserving system resources (via personal authentication system, See the Title and Abstract), comprising the acts of:

activating a first tier biometric sensor to verify the biometric of said individual (via biometrics characteristic data extracting unit 21 for primary verification); and

activating a second tier biometric sensor (characteristic data extracting unit 25) to verify the biometric of said individual in the case where said individual is unsuccessfully verified with said first tier biometric sensor (via verification determining unit 23 determines that the primary verification is insufficient, secondary verifying unit 25 is activated, See S4-S5 on Figure 3). (See Col. 19, lines 53-64; and Col. 20, line 35 - Col. 21, line 22)

Regarding claim 15, Ikegami discloses a system (See the Abstract and Figure 1) comprising:

a biometric security device (authentication system 1) comprising a plurality of biometric devices (via primary verification unit 21 and secondary verification unit 25 in authenticating apparatus 3, Figure 1 and 4);

at least one processor connected to said biometric security device (via authenticating apparatus 3), said at least one processor including one or more databases for storing biometric and user data (via data storage unit 5 and 6, See Figure 3; and Col. 20, line 19 to Col. 21, line 22);

said processor programmed to process the method disclosed in claim 3 above (Therefore, the claimed limitations are rejected for the same reasons as claim 3 above)

Regarding claim 4 and 16, Ikegami discloses said second tier biometric sensor is a comparatively more sophisticated sensor than said first tier biometric sensor (via first sensor may be a fingerprint sensor and the second sensor may be a blood vessel pattern sensor, See the Abstract)

Claim Rejections - 35 USC § 103

7. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

This application currently names joint inventors. In considering patentability of the claims under 35 U.S.C. 103(a), the examiner presumes that the subject matter of the various claims was commonly owned at the time any inventions covered therein

were made absent any evidence to the contrary. Applicant is advised of the obligation under 37 CFR 1.56 to point out the inventor and invention dates of each claim that was not commonly owned at the time a later invention was made in order for the examiner to consider the applicability of 35 U.S.C. 103(c) and potential 35 U.S.C. 102(e), (f) or (g) prior art under 35 U.S.C. 103(a).

8. Claims 5-6 and 17-18 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nikolsky (US 2003/0068044), and further in view of French et al. (US 6,496,936).

Regarding claim 5, Nikolsky discloses a method for selectively activating biometric sensors to authenticate the identity of an individual, comprising:

activating a first tier biometric sensor (via finger print sensor 15, See Figure 1) to verify the biometric of said individual (Paragraph 37); and

activating a second tier biometric sensor to verify the biometric of said individual (via biometric sensor 20, See Figure 1 and paragraph 38).

Nikolsky did not specifically disclose determining whether said individual desires a service level exceeding a predetermined service level threshold; and activating the second tier biometric sensor when it is determined that said individual desires said service level exceeding said threshold.

French teaches a multi-level authentication system to verify users before making access to secure services available to the users. For a low risk service, a simple authentication is sufficient. On the other hand, for a high risk service, a more thorough authentication process is required. (See the Abstract and Col. 3, lines 4-18)

From the teachings of French, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Nikolsky to include determining whether said individual desires a service level exceeding a predetermined service level threshold; and activating the second tier biometric sensor when it is determined that said individual desires said service level exceeding said threshold as taught by French to use a multi-level authentication system to authenticate individuals, thereby providing highly secured services only to individuals that are properly authenticated.

Regarding claim 17, the combination of Nikolsky and French discloses the structural elements of the claimed invention (See rejection on claim 5 above), wherein Nikolsky discloses the system further comprising:

a biometric security device (authentication system 1) comprising a plurality of biometric devices (via primary verification unit 21 and secondary verification unit 25 in authenticating apparatus 3, Figure 1 and 4);

at least one processor connected to said biometric security device (via authenticating apparatus 3), said at least one processor including one or more databases for storing biometric and user data (via data storage unit 5 and 6, See Figure 3; and Col. 20, line 19 to Col. 21, line 22).

Regarding claim 6 and 18, Nikolsky discloses the second tier biometric sensor is more sophisticated than the first biometric sensor (via the biometric sensor to sense distress experienced by a pilot, See paragraph 8).

9. Claims 7-8 and 19-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nikolsky (US 2003/0068044), and further in view of Upton (US 5,864,296).

Regarding claim 7, Nikolsky discloses a method for selectively activating biometric sensors to authenticate the identity of an individual, comprising:

activating a first tier biometric sensor (via finger print sensor 15, See Figure 1) to verify the biometric of said individual (Paragraph 37); and

activating a second tier biometric sensor to verify the biometric of said individual (via biometric sensor 20, See Figure 1 and paragraph 38).

Nikolsky did not specifically disclose determining whether an environmental parameter is outside of a predetermined range; and activating the second tier biometric sensor to verify the biometric of said individual when said environmental parameter is determined to be outside said predetermined range.

Upton teaches a fingerprint detector using a resistance sensor. When the resistance sensor detects contact, the fingerprint detector is immediately activated. (See the Abstract and Col. 7, lines 18-28)

From the teachings of Upton, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Nikolsky to include determining whether an environmental parameter is outside of a predetermined range; and activating the second tier biometric sensor to verify the biometric of said individual when said environmental parameter is determined to be outside said predetermined range as taught by Upton to selectively activate the second biometric sensor only when

an environmental parameter is outside of a predetermined range (resistance is detected to be outside a range).

Regarding claim 19, the combination of Nikolsky and Upton discloses the structural elements of the claimed invention (See rejection on claim 7 above), wherein Nikolsky discloses the system further comprising:

a biometric security device (authentication system 1) comprising a plurality of biometric devices (via primary verification unit 21 and secondary verification unit 25 in authenticating apparatus 3, Figure 1 and 4);

at least one processor connected to said biometric security device (via authenticating apparatus 3), said at least one processor including one or more databases for storing biometric and user data (via data storage unit 5 and 6, See Figure 3; and Col. 20, line 19 to Col. 21, line 22).

Regarding claim 8 and 20, Nikolsky discloses the second tier biometric sensor is more sophisticated than the first biometric sensor (via the biometric sensor to sense distress experienced by a pilot, See paragraph 8).

.

10. Claims 9-12, and 21-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Ikegami et al. (US 6,983,061) and further in view of Epstein (US 2002/0124176).

Regarding claims 9-12, Ikegami discloses the structural elements of the claimed invention (See rejection on claim 3 above), wherein Ikegami further discloses during an enrollment stage, and enrolling said individual with a biometric system using first tier

and second tier biometric sensors (via biometrics characteristic data extracting unit 11 and 14, See Col. 19, lines 47).

Ikegami did not specifically disclose using a magnetic storage medium of a token with identification data stored in order to use the biometric sensors to authenticate an individual.

Epstein teaches the use of biometric information for authentication and access control facilitated by the use of a token device. The token device contains an encryption of a key that is based on an authorized user's biometric information. (See the Abstract)

From the teachings of Epstein, it would have been obvious to one of ordinary skill in the art at the time the invention was made to modify the method of Ikegami to include using a magnetic storage medium of a token with identification data stored as taught by Epstein to increase the security of the authentication system, thereby making the system more secure.

Regarding claim 21, the combination of Ikegami and Epstein discloses the structural elements of the claimed invention, wherein Ikegami further discloses the system, comprising: a biometric security device (authentication system 1) comprising a plurality of biometric devices (via primary verification unit 21 and secondary verification unit 25 in authenticating apparatus 3, Figure 1 and 4);

at least one processor connected to said biometric security device (via authenticating apparatus 3), said at least one processor including one or more databases for storing biometric and user data (via data storage unit 5 and 6, See Figure 3; and Col. 20, line 19 to Col. 21, line 22).

Regarding claim 22, Ikegami discloses said second tier biometric sensor is a comparatively more sophisticated sensor than said first tier biometric sensor (via first sensor may be a fingerprint sensor and the second sensor may be a blood vessel pattern sensor, See the Abstract).

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to YONG HANG JIANG whose telephone number is (571)270-3024. The examiner can normally be reached on M-F 9:30 am to 6:00 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Brian A. Zimmerman can be reached on 571-272-3059. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Y. J./
Examiner, Art Unit 2612

/Brian A Zimmerman/
Supervisory Patent Examiner, Art Unit 2612